PRIVACY FIRST
eigen keuzes in een vrije omgeving

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan	:	European Data Protection Board
Ons ref.	:	SPF20200915NL
Datum	:	16 september 2020
Onderwerp	:	Feedback op de 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR'

1. Inleiding

Geachte leden van de *European Data Protection Board*,

Dit document bevat de reactie van Stichting Privacy First op de Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 1.0, open for Public consultation under reference 06/2020. Stichting Privacy First is een in 2008 opgerichte Nederlandse stichting met ANBI-status,[1] die zich inzet voor het behouden en bevorderen van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving. Vanuit deze achtergrond gaan we in op enkele zaken uit uw concept richtsnoeren.

Stichting Privacy First houdt zich al jaren bezig met financiële privacy. Sinds 2017 zijn we betrokken bij de ontwikkelingen rondom PSD2 en maken ons vanaf het eerste moment zorgen over de privacy van betrokkenen. Vanuit onze rol als NGO voor burgerrechten en privacybescherming richten we ons op privacyzorgen die ontstaan rondom de 'account information service providers' ('AISP').

Eind 2017 dachten we dat betere informatie en transparantie voor betrokkenen voldoende zou zijn. De risico's bleken groter en fundamenteler. Onze zorgen uitten we vervolgens voor een breder publiek tijdens de uitzending van AVROTROS Radar van maandagavond 7 januari 2019.[2] Onze zorgen ten aanzien de PSD2 zijn opgenomen in ons PSD2 project. Via dit project leveren we een bijdrage om positieve verbeteringen aan te brengen in de PSD2 en de uitvoer daarvan zodat betere bescherming van privacy tot stand komt. Informatie over onze inspanningen is breed toegankelijk via onze Nederlands- en Engelstalige website PSD2meniet.nl[3], die informatie bevat over de PSD2, de zorgen die we hierover hebben en oplossingen zoals het PSD2-me-niet register.

Hoewel de PSD2 en de AVG waarborgen bieden om de fundamentele vrijheden en rechten van betrokkenen te beschermen, ligt de daadwerkelijke bescherming van betrokkenen in een juiste uitvoer en interpretatie van de AVG door de rekeninginformatiedienstaanbieders. Uw guidelines hebben dan ook een belangrijke functie.

---

[1] Public Benefit Organisation" (Dutch: *Algemeen Nut Beogende Instelling*, ANBI)
[2] Zie: https://privacyfirst.nl/acties-3/psd2meniet-nl/item/1137-privacy-first-eist-psd2-me-niet-register.html en https://radar.avrotros.nl/uitzendingen/gemist/item/wat-betekent-de-nieuwe-betaalrichtlijn-psd2-voor-jou/ (Nederlands)
[3] https://psd2meniet.nl/en/

We willen u complimenteren met het uitgebreide document dat veel informatie biedt over hoe aanbieders van rekeningdiensten om moeten gaan met hun dienstverlening onder de PSD2. Een aantal begrippen en principes wordt goed uitgewerkt zodat aanbieders van diensten onder de PSD2 zich niet kunnen verschuilen achter een gebrekkige interpretatie van de PSD.

We hebben een aantal algemene suggesties en een aantal specifieke verbeterpunten die mogelijk bijdragen aan betere guidelines.

2. Risico's op hoofdlijnen

Grote verschillen tussen beschermingsregimes PSD2 en AVG

Er is een groot verschil tussen de beschermingsregimes van de PSD2 en de AVG. Het beschermingsregime van de AVG blijkt in de praktijk helaas lager te zijn dan dat van de PSD2. We willen waarschuwen voor papieren waarborgen en vragen aandacht voor het afdwingen van en toezicht houden op privacy by design waardoor risico's voor fundamentele rechten en vrijheden van betrokkenen bij voorbaat worden gemitigeerd of uitgesloten. Betalingsdienstverleners die diensten aanbieden onder de PSD2 zijn gehouden aan uitgebreide vereisten op basis van vergunningen.

Overtreding van de GDPR is weliswaar te sanctioneren, maar zal in haar consequentie niet leiden tot het intrekken van de banklicentie en daarmee het staken van de bedrijfsvoering, maar hooguit tot een boete van ten hoogste €20M of 4% van de wereldwijde omzet.[4] Een relatief lagere sanctie. In de praktijk zullen de boetes zelfs lager zijn, getuige het boetebesluit van de Nederlandse toezichthouder.[5] Daarnaast is het toezicht van de toezichthouders reactief en geen onderdeel van een jaarlijkse terugkerende beoordeling van een licentie.

Volledige controle over persoonsgegevens moet het doel zijn

In punt 1 van uw document geeft u aan dat 'bepaalde vragen en zorgen rijzen met betrekking tot de **noodzaak** dat de betrokkene de **volledige controle** [vet door ons toegevoegd] over hun persoonsgegevens houden.' Uit onze ervaringen wordt helaas duidelijk dat de AVG en alle hiermee samenhangende wetten, regelingen en uitwerking zijn niet in staat zijn dit doel te bereiken. De AVG zal dusdanig in het voordeel van een betrokkene uitgelegd moeten worden dat dit doel wél behaald kan worden. Er is een verregaande vorm van Persoonlijk Data Management (PDM) voor nodig om een persoon volledige controle te geven, waar de betrokkene niet afhankelijk is van de AISP.

Er bestaan inmiddels goede technieken en voorbeelden van toepassingen waarmee een persoon zijn gegevens kan verwerken op zijn of haar eigen smartphone. We wijzen bijvoorbeeld op het initiatieven als 'het Financiële Paspoort" (stichting Financieel Paspoort[6])

[4] Artikel 83 AVG
[5] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan
[6] https://financieelpaspoort.nl/

of het “huurpaspoort”(Qii[7]). Toegang tot iemands eigen gegevens zou de PSD2 ten principale mogelijk moeten maken. Artikel 20 AVG biedt de mogelijkheid van overdracht van gegevens (dataportabiliteit). Dit recht van een betrokkene wordt gehinderd door de PSD2. De PSD2 wetgeving kan in dit inzicht zelfs gedeeltelijk overbodig genoemd worden. De risico’s voor de belangen en rechten van betrokkenen moet dan ook gezien worden in vergelijking met de mogelijkheid informatie te delen zonder derde partij.

Uitoefenen rechten betrokkene nauwelijks mogelijk, mede door profielverrijking

Zodra de gegevens van een betrokkene worden verwerkt door een AISP en deze andere partijen betrekt bij de verwerking, zal het voor een individu vrijwel onmogelijk zijn inzicht te krijgen in de verwerking van zijn of haar gegevens of het verwijderen van gegevens. Zelfs al mocht dit lukken zal het profiel van een persoon verrijkt zijn. Met PSD2 zal profielverrijking nog eenvoudiger gaan en zal een grotere impact hebben dan de losse data die nu verzameld wordt. In coalitie met anderen voert Privacy first een class action op grond van artikel 80 AVG tegen enkele grote partijen waar dit probleem wordt aangekaart.[8]

PSD2 kan risico’s opleveren voor schuldhulpverlening

Een markt waarbij zicht op financiële zaken van belang is, is schuldhulpverlening. In Nederland zijn minimaal 38 (online) boekhoudpakketten beschikbaar die ook aan particulieren worden aangeboden.[9] En 18 online huishoudboekjes.[10] Veel van deze partijen zullen gebruik willen maken van een PSD2-koppeling. Zolang de gegevens worden gebruikt voor de primaire AISP diensten is het risico op onrechtmatige verwerking beperkt. De data maken het echter aantrekkelijk aanvullende diensten aan te bieden. De ervaring leert dat partijen gebruik maken van diensten van derde partijen om te komen tot profilering, online markets om aanbiedingen te doen en risico-en credit scores om risicoprofielen op te zetten. Voor mensen in een kwetsbare positie vanwege schulden zal het gebruiken van AISP’s nauwelijks een vrije keuze zijn. Datzelfde geldt voor aangeboden aanvullende diensten. Onze stelling is dan ook, ‘eens gegeven blijft gegeven’. Het is van belang dat vóórdat gegevens worden gedeeld risico’s weggenomen zijn en betrokkenen maximale bescherming is geboden.

Privacy dienstverlening moet op zelfde niveau commerciële dienstverlening zitten

De AVG biedt het kader voor de verwerking van persoonsgegevens. Een groot aantal wettelijke bepalingen moet door de verwerkingsverantwoordelijke worden vertaald naar diens eigen organisatie. De inrichting van de organisatie moet de AVG dusdanig interpreteren dat deze de fundamentele rechten en vrijheden van betrokkenen waarborgt. De privacy-gerelateerde dienstverlening moet op vergelijkbaar niveau zijn als de andere dienstverlening, om te voorkomen dat het uitoefenen van rechten moeilijker is en daarmee een drempel voor het uitoefenen ontstaat. Het beëindigen van een contract moet net zo eenvoudig zijn als het aangaan van een overeenkomst.

---

[7] https://qii.nl/
[8] https://www.privacyfirst.eu/focus-areas/online-privacy/689-the-privacy-collective-takes-oracle-and-salesforce-to-court.html
[9] https://www.boekhoudeninexcel.nl/verdien-200-euro-per-jaar-met-de-besparingschecker/
[10] Consumentenbond, 31 maart 2020, 'Digitale huishoudboekjes', https://www.consumentenbond.nl/budgetteren/digitale-huishoudboekjes

3. Algemeen

Conform artikel 108 PSD2 evalueert de Commissie de richtlijn per 13 januari 2021. We spreken de wens uit dat waar mogelijk elementen van de richtsnoeren in de wet verankerd worden, bijvoorbeeld door het opnemen van een verwijzing naar dit advies of opname van bepalingen in de toelichting bij artikelen.

I. ***Suggestie***: Informeer de Europese Commissie over deze Richtsnoeren en laat ze, samen met inzichten die u opdoet tijdens de consultatie, onderdeel zijn van de evaluatie van de PSD2.

In onze opinie ontstaan ten aanzien van privacy de grootste risico's voor betrokkenen op het moment dat een AISP aanvullende diensten wil gaan aanbieden, of dat een dienstverlener gebruik wil gaan maken van AISP diensten en hiervoor een derde partij aantrekt. Het zal hier gaan om een verdere verwerking van persoonsgegevens of nieuwe diensten. Het vertrekpunt is dan wanneer een betrokkene een nieuwe contractuele relatie aangaat. Omdat al sprake is van een relatie, zal de drempel en daarmee de waarborgen in deze gevallen lager zijn en de aanbieder heeft meer mogelijkheden om het gedrag van de consument te beïnvloeden.

Deze mogelijkheid van een verdere verwerking beschrijft u in paragraaf 2.3, de punten 20 tot en met 24. Deze mogelijkheid is dan ook de primaire focus van onze inspanningen en deze evaluatie. Op dat moment kunnen transactiegegevens gebruikt worden voor aanvullende verwerkingen van persoonsgegevens op grond van artikel 5 lid 1 sub b en artikel 6 lid 4 AVG. Voor AISP's zit hier de werkelijke waarde van de PSD2 en kunnen nieuwe business modellen ontstaan met transactiedata als grondstof. De PSD2 biedt de mogelijkheden om financiële data te koppelen aan andere data. Transactiedata geven een volledig en diepgaand profiel van een betrokkene.

II. ***Suggestie***: benadruk dat verwerkingsverantwoordelijken en verwerkers de AVG ten gunste van betrokkenen moeten uitleggen. Termijnen rondom de rechten van betrokkenen (artikel 15 en verder AVG) zijn maximum termijnen waar slechts bij hoge uitzondering gebruik van wordt gemaakt.
III. ***Suggestie:*** Benadruk dat de aan privacy gerelateerde elementen van zowel de PSD2 als de AVG uitgelegd moeten worden en dat een betrokkene volledige controle heeft over diens persoonsgegevens. Dat houdt in dat iedere vertraging in het uitoefenen van rechten, tekort schietende communicatie of tactieken waardoor consumenten keuzes maken die ze op later moment betreuren, de verwerking van persoonsgegevens onrechtmatig maakt.
IV. ***Suggestie:*** geef aan op welke momenten risico's voor betrokkenen ontstaan of verwijs naar een in het kader van de PSD2 uitgevoerde DPIA waarin deze risico's zijn benoemd.

Het Comité zal in overweging moeten nemen dat de PSD2 ten principale nieuwe risico's doet ontstaan. Een kernprobleem van de nieuwe mogelijkheden van de PSD2 ligt in het gebruik van een *third party* zoals een AISP. Wanneer een persoon drie bankaccounts heeft en deze in

één overzicht wil hebben, zal de betrokkene gebruik moeten maken van de diensten van een derde partij, de AISP.[11] Daarmee komt deze tussen de communicatie te staan tussen een consument en een bank. De wet zou mogelijk moeten maken dat een persoon conform artikel 67 lid 1 toegang krijgt tot al zijn gegevens in een andere omgeving dan die van de bank, echter zónder dat hierbij een derde partij als verwerkende partij betrokken is. De PSD2 creëert weliswaar een nieuwe mogelijkheid, maar creëert tegelijk een nieuw risico door deze derde partij te verplichten.

V. ***Suggestie***: overweeg bij het opstellen van guidelines en het houden van toezicht het alternatief waarbij een consument toegang krijgt tot zijn betalingsgegevens echter zonder dat daarvoor een derde partij zoals een AISP betrokken moet zijn.

Consumenten kunnen de hoeveelheid bankgegevens niet beperken. Zelfs als een financiële dienstverlener deze gegevens niet nodig heeft, wordt na het geven van toestemming toch alle data gedeeld. Dit is in strijd met het principe van dataminimalisatie onder de AVG. Uw guidelines kunnen versterkt worden door deze te voorzien van enkele voorbeelden. Voorbeelden zijn: beperkingen in de duur waarover gegevens worden gedeeld. Onderscheid maken tussen inkomsten en uitgaven. Het kunnen uitsluiten van bepaalde waarden voordat zij verder worden verwerkt.

VI. ***Suggestie***: gebruik voorbeelden van toepassingen om grenzen van verwerkingen te illustreren.

[11] Zie overweging 28 PSD2 waar dit voorbeeld op is gebaseerd.

4. Transparantie en informatie

In uw hoofdstuk 6.4 van de concept richtlijnen gaat u in op transparantie en verantwoording. Op dit moment worden consumenten onvoldoende goed en eerlijk voorgelicht. Veel verstrekte informatie is vaak moeilijk leesbaar. Een kwalijke zaak, zeker omdat aan hun uitdrukkelijke toestemming veel waarde wordt gehecht. Maar hoeveel waarde heeft toestemming als een consument consequenties van het geven van toestemming onvoldoende kan inschatten?

De roep om duidelijke informatie blijft niet beperkt tot deze financiële informatie. Een consument die gebruik wil maken van een AISP deelt zijn of haar gegevens met een derde partij. Het gaat om zoveel informatie als beschikbaar is bij de betalingsdienstverlener. Het gaat om veel informatie. Met één druk op de knop deelt een persoon een volledige financiële geschiedenis. Uit onderzoek van de Nederlandse Consumentenbond bleek dat men bij Nederlandse banken gemiddeld zeven jaar kan terugkijken.[12] Enkele banken laten tot twee jaar terugzien, nieuwere banken hebben geen maximumtermijn meer en kunnen op termijn een leven lang aan transacties bevatten.

Door gebruik te maken van diensten voor verdere verwerkingen zoals credit scoring of anderen vormen van risico-indicatie kan een derde partij op basis van die informatie een diepgaande analyse van een persoon maken. Overigens sluiten wij niet uit dat AISP's ook voor een 'geconsolideerde weergave' gebruik zullen maken van derde partijen, waaronder kredietbeoordelaren.

In plaats van de positie van de EDBP te beperken tot het bieden van de wettelijk verplichte informatie verdient het aanbeveling dat de EDPB aanbieders wijst op het belang en nut van informatie. Daarbij is begrip van de verwerking, risico's en zicht op de aard en omvang van de verwerking van belang.

Bij uw punt 8 en 10 noemt u de vrijwilligheid van een persoon om gebruik te maken van een dienst. Het ligt in de lijn der verwachting dat aanbieders van financiële diensten hun diensten zullen specificeren naar het wel of niet gebruik van een PSD2 koppeling voor kredietbeoordelingen. Deze specificatie zal alleen toegestaan moeten worden wanneer een aanbieder voldoende waarborgen biedt in de vorm van het voorkomen van profilering, het niet toevoegen van datasets aan andere informatie van de persoon en strikte dataminimalisatie. Zelfs onder deze voorwaarden is de scheidslijn tussen 'verleiden', 'zachte dwang' en 'onvrijwillig' zeer dun.

Een ontwikkeling die ontstaat door de PSD2 is dat dienstverleners voor hun financiële ondersteuning gebruik gaan maken van dienstverleners onder de PSD2. In de praktijk kwamen we een casus tegen van een penningmeester van een sportvereniging die zich afvroeg of hij moest instemmen met het gebruik van een PSD2 dienstverlener voor het innen van contributie. Uit onderzoek bleek dat de sportvereniging verwees naar het privacy statement van een derde partij, die vervolgens wederverkoper bleek te zijn van de

[12] Consumentenbond, 9 mei 2018, 'Meerderheid bewaart rekeningafschriften ten minste 5 jaar', https://www.consumentenbond.nl/betaalrekening/meerderheid-bewaart-rekeningafschriften-ten-minste-5-jaar

uiteindelijke verwerker. Dergelijke constructies verwachten we steeds vaker aan te treffen omdat dienstverleners betalingsdiensten zullen inkopen bij gelicentieerde partijen. Het wordt voor de doorsnee betrokkene onmogelijk een goed beeld te krijgen door wie zijn persoonsgegevens worden verwerkt.

Het Comité zal bij het schrijven van haar guidelines voor het ondersteunen van de toezichthoudende taken moeten beseffen dat Privacy statements te lang en moeilijk te doorgronden zijn. Bij ons eigen onderzoek naar de privacy statements van Yolt, Spiir en Google Pay zagen we dat het aantal pagina's waar het privacy statement uit bestaat respectievelijk 8, 13 en 4 was, waarbij Google Pay haar voorwaarden verbindt aan de algemene voorwaarden van 31 pagina's. De onderzochte privacy statements hadden allen een andere opzet en opmaak. Ze helpen consumenten niet bij het kunnen beoordelen van de informatie.

Artikel 12 AVG stelt dat informatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal moet worden verstrekt. De praktijk leert dat informatie vaak niet volgens deze normen wordt verstrekt.

VII. ***Suggestie***: bevestig dat informatie verstrekt moet worden conform de eisen zoals gesteld in artikel 12 AVG.

De EDPB zou aandacht kunnen schenken aan instrumenten waarmee de informatieplicht laagdrempelig wordt ingevuld. De AVG biedt hiervoor een mogelijkheid in artikel 12 lid 7. In dit artikel wordt duidelijk gemaakt dat de in artikel 13 en 14 AVG te verstrekken informatie ook middels icoontjes gedeeld mag worden. Logischerwijs mogen dit ook vergelijkbare, communicatief eenvoudige en makkelijk toegankelijke alternatieven zijn. De EDBP zou zich kunnen inzetten om dit artikel onder de aandacht te brengen. Bij de icoontjes wordt genoemd dat deze machine leesbaar zijn. Wanneer icoontjes machine leesbaar zijn kunnen ze doorsoftware geïnterpreteerd worden waarmee nieuwe diensten kunnen ontstaan.

VIII. ***Suggestie***: benadruk dat aanbieders van betalingsdiensten informatie eenvoudig moeten bieden. Benoem de mogelijkheid van artikel 12 lid 7 AVG waarbij de mogelijkheid van icoontjes wordt benoemd.

IX. ***Suggestie***: benadruk de mogelijkheid die naast de icoontjes van artikel 12 lid 7 wordt benoemd, namelijk dat informatie machine readable is. Dat opent de mogelijkheid voor onderlinge vergelijkbaarheid van informatie tussen aanbieders.

We willen benadrukken dat ook communicatie en communicatietechnieken zich ontwikkelen. Een voorbeeld hiervan is microtargetting en neuromarketing. De manier waarop informatie wordt gegeven en transparant wordt gecommuniceerd, zou net als bij het gegevensbeschermingsbeleid zoals verwoord in artikel 24 en 32 AVG passend zijn en moeten aansluiten bij de stand van de techniek. Vergelijkbaar met de 'best practices' voor

informatiebeveiliging[13] mag dit ook van toepassing worden verklaard op communicatie. We wijzen erop dat moderne communicatie technieken worden ingezet om de diensten onder de aandacht te brengen en hen in een bevoordeelde positie brengen. Om een balans te brengen in technieken en informatie zal u hier aandacht voor moeten vragen in uw guidelines.

Een voorbeeld van een vorm van presentatie biedt het Privacy Label.[14] Middels dit label is inzichtelijk te maken wat de belangrijkste elementen van de verwerking van persoonsgegevens zijn. Daarnaast is die informatie machine-leesbaar en daardoor wordt de informatie geschikt voor nader gebruik.

X. ***Suggestie***: besef dat instrumenten bestaan waarmee informatie toegankelijk gepresenteerd kan worden en gezien moeten worden als 'stand van de techniek' op het gebied van communicatie.

XI. ***Suggestie***: benadruk dat communicatiemiddelen rondom rechten en vrijheden van betrokkenen in balans moeten zijn met communicatiemiddelen die worden benut om commerciële diensten onder de aandacht te brengen. Benadruk dat aanbieders hier een faire balans in moeten aanbrengen.

XII. ***Suggestie***: neem de methode van het Privacy Label over als voorbeeld van een aanpak om op toegankelijke, bondige en eenvoudige wijze te voorzien in de informatieplichten van de AVG.

Een ander voorbeeld wordt gedragen door het Dutch National Forum on the Payment System (Nederlands Maatschappelijk overleg betalingsverkeer (MOB)).[15] Deze heeft in zijn vergadering van 26 mei 2020 ingestemd met de 'good practice rekeninginformatiedienstverlening'[16] om transparantie over rekeninginformatiediensten op grond van PSD2 te krijgen. Om dit te bevorderen heeft het MOB een good practice opgesteld waarin zeven vragen zijn opgenomen aan rekeninginformatiedienstverleners om voor het moment dat de gebruiker toestemming geeft aan de aanbieder voor toegang tot zijn of haar rekening, bondig en begrijpelijk te beantwoorden. Belangrijk is te beseffen dat deze vragen zijn opgesteld door consumenten. Ze overlappen met de informatieplichten uit artikel 13 en 14 AVG, maar zijn bondiger en meer gericht op de informatiebehoefte van de consument. Deze vragen komen naast de informatieplichten. De vragen zijn:

1. Wie vraagt toegang tot mijn rekeninginformatie? Hoe is de dienst gereguleerd?
2. Welke dienst biedt <naam van de aanbieder> aan waar mijn data voor nodig is?
3. Welke gegevens van mijn rekening gaat <naam van de aanbieder> gebruiken?
4. Waarvoor gebruikt <naam van de aanbieder> de gegevens nog meer?
5. Welke gegevens gaan naar derden en waarvoor?

---

[13] 'What is "state of the art" in IT security?'ENISA and TeleTrusT - IT Security Association Germany have, February 07, 2019 (https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/)

[14] https://www.privacylabel.org/learn/

[15] https://www.dnb.nl/en/payments/other-tasks/national-forum-on-the-payment-system/index.jsp

[16] See for the press statement including attachements the site of the DNB: https://www.dnb.nl/en/news/news-and-archive/nieuws-2020/dnb388945.jsp

6. Hoe kan ik mijn eerder gegeven toestemming terugdraaien?
7. Waar is verdere informatie te vinden?

XIII. ***Suggestie***: neem de best practices van het Dutch National Forum on the Payment System over als voorbeeld van een aanpak om consumenten te voorzien in hun informatiebehoefte.

Om informatie en transparantie te verbeteren kunt u verwijzen naar andere thema's in de financiële dienstverlening. Informatie over financiële diensten begrijpen is lastig en behaalt vaak niet het beoogde doel. In juli 2019 promoveerde Dr. C. de Jager op haar proefschrift waarin ze aangeeft dat financiële bijsluiters voor klanten vaak moeilijk te begrijpen zijn onder meer door technisch taalgebruik en daardoor hun doel voorbijschieten.[17] Inmiddels wordt gebruik gemaakt van een Europees informatiedocument, het Key Information Document op grond van Verordening (EU) Nr. 1286/2014 van het Europees parlement en de Raad van 26 november 2014 over essentiële-informatiedocumenten voor verpakte retailbeleggingsproducten en verzekering gebaseerde beleggingsproducten (PRIIP's).

In antwoord op vragen van het Nederlandse Parlement benoemde de minister het nut van goede informatie, in relatie tot het KID: "Om de leesbaarheid van het KID te vergroten, moet het KID een op zichzelf staand document zijn en mag het geen verwijzingen bevatten naar marketing-materiaal. Om de leesbaarheid van het KID verder te vergroten, wordt in het KID deels gebruik gemaakt van voorgeschreven teksten of figuren die verplicht in het document moeten worden opgenomen. Ten slotte dient het KID, anders dan bij de financiële bijsluiter het geval was, aan de consument te worden verstrekt vóórdat deze consument door een overeenkomst of aanbod met betrekking tot dat product is gebonden. Hiermee wordt beoogd de consument tijd te geven om een beter inzicht te krijgen in de risico's, kosten en het beoogd rendement." De Europese Commissie zal het KID evalueren en daarbij mede kijken of het bijdraagt aan een beter begrip van de financiële dienst.

XIV. ***Suggestie***: adviseer transparantie en informatie naar betrokkenen in te richten op vergelijkbare wijzen als op andere thema's in de financiële sector gebruikelijk is, bijvoorbeeld bij het Europees informatiedocument, het Key Information Document.

In punt 74. geeft u aan dat de betrokkene met name geïnformeerd moet worden over de periode waarin de persoonsgegevens worden opgeslagen. Onder deze informatie hoort logischerwijs ook opgenomen te worden hoe de aanbieder omgaat met gegevens zodra een contract wordt ontbonden, of toestemming onder de gegevensoverdracht naar een AISP niet wordt verlengd, of een gegeven toestemming onder artikel 94 lid 2 PSD2 binnen 90 dagen wordt ingetrokken.

XV. ***Suggestie***: neem bij punt 74 op dat een aanbieder aan dient te geven hoe deze om gaat met persoonsgegevens zodra een contract wordt ontbonden, of toestemming onder de

[17] Jager, C. de (2018), 'Consumentenbescherming door informatie?' (Proefschrift RUG)

gegevensoverdracht naar een AISP niet wordt verlengd, of een gegeven toestemming onder artikel 94 lid 2 PSD2 binnen 90 dagen wordt ingetrokken.

XVI. ***Suggestie***: verbijzonder bij punt 75 het moment in uw aanwijzing "op dat de informatie uiterlijk op het moment van 'de eerste communicatie' moet plaats vinden". Logischerwijs vindt deze plaats voordat een contract wordt afgesloten.

Uw Richtsnoeren kunnen bijdragen aan betere informatievoorziening door een uitspraak te doen over het moment van informeren. De AVG gaat uit van informeren voordat een verwerking begint. Omdat de PSD2 uitgaat van een contractuele relatie, zal een persoon al bij het afwegen van het aangaan van een contract, informatie moeten bezitten om deze afweging te maken. In dat licht is het opvallend dat informatie over een bepaalde dienst niet altijd te vinden is. Informatie over de diensten zelf is vaak alleen te ontvangen zodra een persoon een dienst gaat afnemen, of een app downloadt uit een Google App store of Apple App store. De EDPB kan adviseren om informatie over dergelijke specifieke diensten ook op een algemeen toegankelijke website te plaatsen en deze informatie te laten aansluiten op de informatie die een consument wel krijgt tijdens het aanschaffen van een dienst.

XVII. ***Suggestie:*** benoem dat het verstrekken van informatie in het kader van de informatie- en transparantieplicht onder artikel 12 AVG, tijdig moet gebeuren. Dit houdt in gedurende het keuzeproces of een persoon zijn of haar toestemming wil geven. Wanneer een persoon te laat wordt geïnformeerd zullen toezichthouders de toestemming als niet rechtmatig moeten beschouwen.

5. Expliciete Toestemming

We gaan in op uw document onder hoofdstuk 3, uitdrukkelijke toestemming. Net als in uw brief van 2018 geeft u aan dat uitdrukkelijke toestemming onder de PSD2, gegeven in artikel 94 lid 2 gezien moet worden in de contractuele context. U concludeert bij punt 43 dat expliciete toestemming in het kader van de PSD2 niet hetzelfde is als (expliciete) toestemming in het kader van de AVG. Het verschil is dat toestemming onder de AVG een grondslag onder artikel 6 AVG verschaft en uitdrukkelijke toestemming onder de PSD2 een aanvullende vereiste van contractuele aard.

Wat niet duidelijk is, is of de toestemming zoals bedoeld in de PSD2 wel moet voldoen aan alle eisen en criteria die gelden voor toestemming onder de AVG. Daarnaast noemt u een aantal elementen op waar toestemming onder de PSD2 aan moet voldoen, maar maakt niet duidelijk of deze volledig overeenkomen aan de eisen die aan toestemming onder de AVG worden gesteld, of waarin deze verschillen.

XVIII. ***Suggestie:*** bevestig of verduidelijk overeenkomsten en verschillen tussen de eisen aan toestemming onder de AVG en de PSD2.

Centraal staat dat toestemming binnen de AVG een 'vrijelijk gegeven, specifieke, geïnformeerde en ondubbelzinnige aanduiding van de wensen van de betrokkene is waarmee hij of zij, door middel van een verklaring of duidelijke positieve handeling, instemt met de verwerking van hem of haar betreffende persoonsgegevens." Deze vier elementen zijn essentieel voor een geldige toestemming.

De AVG hanteert de term 'geïnformeerd' als onderdeel van een geldige toestemming. Doorgaans wordt dit ten onrechte geïnterpreteerd als het simpelweg verstrekken van de wettelijk vereiste informatie aan de betrokkene, waarmee de verwerkingsverantwoordelijke aan zijn verantwoordelijkheid heeft voldaan. Het effect dat de AVG beoogt is dat een persoon op basis van informatie een weloverwogen keuze kan maken over de verwerking van zijn of haar persoonsgegevens. In het geval van PSD2 wordt dit uitgangspunt ondergraven. Inmiddels kan nauwelijks meer gesproken worden over geïnformeerde betrokkene, omdat de reikwijdte van de gegeven toestemming niet meer overzien kan worden. Het effect zal zijn dat een persoon weliswaar weet dát toestemming is gegeven, maar nauwelijks zal kunnen aangeven wat de verwerking, naar aard en omvang, inhoudt en welke risico's voor zijn of haar fundamentele rechten vrijheden ontstaan.

Bij het adviseren van toezichthouders en aanbieders van PSD2 diensten is het goed te beseffen dat het geven van informatie niet automatisch betekent dat een persoon de omvang en mogelijkheden die de aanbieder heeft kan overzien. Zeker zodra een AISP verdere verwerkingen uitvoert of laat voeren zal een betrokkene moeilijk de impact van het delen van een volledig financieel profiel kunnen inschatten.

XIX. ***Suggestie:*** leg beter uit wat het doel van geïnformeerde toestemming moet zijn, wat een betrokkene mag verwachten en hoe een aanbieder kan nagaan of een betrokkene beseft waar deze toestemming voor heeft gegeven.

Toestemming is ten aanzien van het verstrekken van gegevens door consumenten een belangrijke waarborg binnen de PSD2. Niet duidelijk is of de wetgever de uitdrukkelijke toestemming als waarborg ziet. Deze wordt echter wel zo gepresenteerd door DNB en Nederlandse banken. In de concept richtsnoeren gaat de EDPB niet in op het intrekken van toestemming. Iedere 90 dagen moet een toestemming worden herbevestigd. Wanneer een persoon zijn of haar toestemming niet verlengd, mogen geen gegevens verwerkt worden en wordt het account inactief.

Logisch beredeneert eindigt de grondslag onder de verwerking na het actief intrekken van toestemming. De betrokkene zal aangeboden moeten worden zijn gegevens te wissen zodat recht wordt gedaan aan artikel 5 lid 1 sub 3 en 17 AVG. Het bewaren van gegevens nadat toestemming is ingetrokken houdt de verwerking in stand en leidt tot schending van de principes van de AVG.

Wanneer een persoon zijn of haar toestemming tijdens de 90 dagen intrekt is sprake van een 'ondubbelzinnige wens' van de betrokkene. Te verwachten zou zijn dat de gevolgen van toestemming twee kanten op gaan. Het intrekken van toestemming blijft nu zonder gevolgen, terwijl de verwerking van persoonsgegevens doorgaat. Het is aan te bevelen dat, zodra een persoon zijn of haar toestemming intrekt, de mogelijkheid wordt geboden direct een verzoek tot gegevenswissing op grond van artikel 17 AVG in te dienen, waar dan direct gevolg aan moet worden geven. Overigens zou een partij hiertoe zelf moeten besluiten daar met het intrekken van de toestemming de grondslag onder de verwerking wegvalt. Het directe consequentie van het intrekken van iemands toestemming, namelijk gegevenswissing, wordt niet behandeld. Voor ons volgt uit het ene het andere., waarbij minimaal is gewenst dat de betrokkene de mogelijkheid tot gegevenswissing wordt geboden.

XX. ***Suggestie:*** werk beter uit wat van een aanbieder verwacht wordt zodra een betrokkene zijn toestemming onder artikel 94 lid 2 AVG intrekt. Benoem hier ook consequenties voor gegevens die nog bewaard worden, onderdeel zijn van interne bedrijfsvoering, profielen, statistieken. Benoem de rechten die een persoon heeft en die door het intrekken van de toestemming ‘geactiveerd’ behoren te worden, met name artikel 17 AVG (gegevenswissing).

Bij uw punt 31 verwijst u naar de EDPB-richtsnoeren 05/2020 waarin staat dat een ondertekening van een schriftelijke verklaring een goede manier is om toestemming te geven. In het geval van PSD2 lijkt het beter aan te sluiten bij authenticatie vormen die in de bancaire wereld bekend zijn, zoals het accorderen via een two-factor authentication of via de portal van de betreffende ASPSP.

XXI. ***Suggestie:*** benoem naast een schriftelijke verklaring ook digitale middelen waarmee een gegeven toestemming aantoonbaar gemaakt kan worden volgens artikel 7 AVG.

Uw punt 34 maakt helaas niet duidelijk hoe de uitzondering van artikel 33 PSD2 werkt. We wijzen er op dat de uitdrukkelijke toestemming van artikel 94 lid 2 PSD2 vaak is genoemd als

waarborg. Artikel 33 PSD2 zondert AISP's uit van deze toestemming, maar niet de dienstverlening. Niet duidelijk is waarom dit is en wat het materiele effect hiervan is. Het holt schijnbaar de waarborg van artikel 94 lid 2 PSD2. Het laatste deel van uw punt 38, in samenhang met punt 39 maakt de samenhang niet duidelijk. Ten aanzien uw punt over de 'centrale overweging dat de betrokkene van tevoren moet kunnen bepalen wat de omvang en de gevolgen van de verwerking zijn en dat hij niet op een later tijdstip mag worden verrast over de wijze waarop zijn persoonsgegevens zijn gebruikt' verwijzen wij u naar onze inbreng over transparantie en informatie.

XXII. ***Suggestie:*** verduidelijk de samenhang tussen uw punt 34 van de concept richtsnoeren in relatie tot de uitzondering van artikel 33 PSD2 op artikel 94 lid 2.

Bij uw punt 30. Het verwerken van bijzondere categorieën persoonsgegevens is in beginsel verboden. Er bestaan uitzonderingen waarbij de uitdrukkelijke toestemming van artikel 9 lid 2 sub a AVG naar alle waarschijnlijkheid de enige uitzonderingsgrond is. Dit punt hangt samen met uw punten 40 en 42. U merkt op dat het mogelijk moet zijn om gebruik te maken van een dienst, zonder categorieën van bijzondere persoonsgegevens te delen. Dit is vergelijkbaar met het aanbieden van verschillende diensten, waarbij het onthouden van toestemming geen negatief effect mag hebben op het gebruik van de dienst.

Bij bijzondere persoonsgegevens dreigt dit wel te gebeuren. Toestemming voor het gebruik van bijzondere persoonsgegevens zien we terugkomen in enkele vormen: a) bijzondere persoonsgegeven worden niet benoemd. b) persoonsgegevens worden als onderdeel gezien van het geheel, dus wie zijn of haar bijzondere persoonsgegevens wil beschermen, zal af moeten zien van de gehele dienst. Daarmee zal de persoon niet kunnen genieten van de mogelijkheden die de wetgever beoogt te geven. Veel personen zullen alsnog hun toestemming geven, terwijl ze een andere keuze zouden maken als het mogelijk was een dienst af te nemen zonder bijzondere persoonsgegevens te verstrekken. De omgang met bijzondere persoonsgegevens vallen wat ons betreft al snel in de categorie 'take it or leave it', zoals u afwijst bij uw punt 18.

Een voorbeeld van deze praktijk is te vinden bij een AISP[18] "Please be aware that if you do not want us to process the data for the purposes set out above, that we cannot deliver you our services." Deze partij vraagt toestemming voor zes verwerkingsdoelen, evenals voor een gerechtvaardigd belang waaronder 26 subdoelen hangen.

Het geven van toestemming voor de verwerking van bijzondere persoonsgegevens raakt met het uitgangspunt dat toestemming 'vrijelijk' gegeven moet worden. Bijzondere persoonsgegevens maken slechts een zeer klein deel uit van het geheel van transactiedata. Het zal moeilijk in te schatten zijn welke negatieve effecten de verwerking van deze persoonsgegevens zal hebben voor een persoon. Echter, de bescherming van bijzondere persoonsgegevens zit niet alleen in de particuliere data zelf, maar ook in het principiële uitgangspunt dat deze gegevens extra bescherming verdienen.

[18] www.yolt.com/privacy, 1 september 2020

XXIII. ***Suggestie***: benadruk bij uw punten 30 en 42 dat een persoon die toestemming wil geven op grond van artikel 94 lid 2 PSD2, maar deze wil onthouden voor de bijzondere persoonsgegevens, toch gebruik moet kunnen maken van de verleende dienst. Zeker wanneer het een verdere verwerking als bedoeld in artikel 5 lid 1 sub b AVG betreft.

6. Verwerking van stilzwijgende partij gegevens (‘silent third party’)

In de bankgegevens van een consument staan ook de gegevens van andermans tegenrekening, dit is de ‘silent third party’. Deze persoon weet niet dat zijn gegevens gedeeld worden en kan dit ook niet verhinderen. Doordat de transactiedata via Big Data en data-analyses veel breder geanalyseerd zullen worden dan voor de inwerkingtreding van PSD2 ontstaan grote risico’s op privacyschendingen. Uw brief van juni 2018 aan het Europees Parlement kwam over als een juridische oplossing voor een fundamenteel probleem. We zijn dan ook blij dat de huidige concept richtsnoeren dieper ingaan op de materie. Toch benoemen de richtsnoeren het fundamentele probleem te weinig.

Net als bij de bijzondere categorieën persoonsgegevens is het kunnen filteren van gegevens van stilzwijgende partijen het uitgangspunt. Ten principale zal een persoon die onderdeel is van een transactie, zich er van verzekerd moeten zijn dat diens gegevens niet opgenomen zijn in verwerkingen waar deze niet bij betrokken is en geen rechten op kan uitoefenen. Voor aanbieders van PISP en AISP diensten geldt een gerechtvaardigd belang bij het verwerken van de gehele transactie. Desondanks leidt de ongelijkheid van rechten tot ongewenste effecten. Aanbevolen moet worden aan aanbieders van diensten op grond van de PSD2 om de mogelijkheid te bieden om geen gegevens van stilzwijgende partijen te verwerken. Duidelijk moet zijn dat de verwerking ontstaat door het karakter van een transactie waarbij twee partijen betrokken zijn en de verwerking van gegevens van de stilzwijgende partij een moeilijk te vermijden bijvangst is. Dat ontslaat verwerkende partijen niet van de plicht om direct na ontvangst van de persoonsgegevens maatregelen te nemen om de verwerking te beperken.

Betrokkene zouden het recht moeten hebben om, met een beroep op artikel 18 AVG, op voorhand bezwaar te maken tegen de verwerking van hun gegevens door dienstverleners op grond van de PSD2. Aanbieders kunnen maatregelen treffen in algemene zin, of aan individuen de mogelijkheid bieden hun rekeningnummer uit te sluiten van bepaalde diensten. Betrokkenen zouden hun voorkeur kunnen opnemen bij hun bank of in een andere vorm van Persoonlijk Datamanagement (PDM) toepassing.

Het gaat hier vooral over het verder verwerken van de gegevens. Het is door aanbieders van kredietbeoordelingen, bedrijven die zich specialiseren in profilering of in risicobeoordelingen, mogelijk om door de grote hoeveelheden data die zij verwerken gegevens van stilzwijgende personen te verwerken en uiteindelijk te verbinden aan het profiel van deze stilzwijgende persoon.

Bij paragraaf 4.1, punt 48 en 49 lijkt het Comité te stellen dat persoonsgegevens van de stilzwijgende partij niet verder verwerkt mogen worden. De paragraaf lijkt hier toch ruimte voor te geven. Het Comité kan duidelijker opnemen dat de gegevens van stilzwijgende partijen niet verder verwerkt mogen worden, afgezien van een wettelijke verplichting. De aanbieders zal hier maatregelen voor moeten treffen.

XXIV. ***Suggestie***: beschrijft duidelijker dat het verder verwerken van gegevens van een stilzwijgende partij niet is toegestaan. Noem daarbij met name het verwerken van deze gegevens voor profileren of construeren van profielen, verrijken van bestaande data en ontwikkelen van netwerkprofielen.

XXV. ***Suggestie***: wijs aanbieders erop dat zij technische en organisatorische maatregelen moeten treffen om verdere verwerking op grond van een gerechtvaardigd belang te voorkomen.

7. Verwerking van bijzondere categorieën van persoonsgegevens in het kader van de PSD2

Bankgegevens bevatten 'bijzondere categorieën persoonsgegevens' die alleen onder strikte voorwaarden verwerkt mogen worden. Een contributiebetaling aan een vakbond, politieke partij of organisatie die seksuele voorkeur onthult, moet gezien worden als bijzonder (gevoelig) persoonsgegeven. Ook transacties met zorgverleners en apotheken moeten als bijzondere persoonsgegevens worden gezien. Op dit moment bestaat geen mogelijkheid deze gegevens te filteren en worden ze verstrekt aan partijen die deze gegevens niet mogen verwerken. Wat Privacy First betreft is er geen reden om aan consumenten geen mogelijkheid tot beperking te bieden. Inmiddels bestaat een oplossing die het filteren van deze data mogelijk maakt, en die als uitgangspunt voor verder toezicht gehanteerd moet worden.

Privacy First is blij met uw beschrijving van punt 51. De rol van bijzondere persoonsgegevens en het feit dat deze afgeleid kunnen worden uit transacties lijkt lange tijd onderbelicht te zijn. We verwelkomen uw punten 56 en 57. Daarbij wijzen we op andere secties in deze bijdrage over de toestemming. We vragen ons af of de beoogde kwaliteit van toestemming wel gehaald wordt binnen PSD2. Voor bijzondere categorieën persoonsgegevens is dit extra risicovol.

In uw punt 52 geeft u aan dat partijen moeten onderzoeken om de verwerking van bepaalde gegevenspunten te verhinderen. Een mogelijkheid die u noemt is het uitvoeren van de DPIA. Hoewel we niet bestrijden dat een DPIA conform artikel 35 AVG bijzondere persoonsgegevens kan identificeren, is dit instrument onvoldoende voor het doel. Zowel het Comité als de Europese Commissie kunnen hier een betere rol spelen. De kern is dat een dienstaanbieder mogelijk niet weet en geen incentive heeft om te onderzoeken in welke gevallen sprake is van een bijzonder persoonsgegeven. Wanneer deze transactiegegevens verwerkt worden, zal de dienstverlener mogelijk niet beseffen of willen beseffen dat de transactie een bijzonder persoonsgegeven onthult. Ook bestaat het risico dat een aanbieder het risico op schending van de rechten en vrijheden van een betrokkene te laag inschat, bijvoorbeeld omdat het gaat om een zeer klein aantal transacties in relatie tot het geheel van transacties.

XXVI. ***Suggestie***: benadruk dat wanneer een DPIA uitwijst dat bijzondere categorieën van persoonsgegevens worden verwerkt, dit direct al aanleiding geeft tot het treffen van maatregelen.

Op PSD2meniet.nl/en is uitgewerkt hoe een PSD2 dienstverlener kan nagaan dat sprake is van een bijzondere categorie van persoonsgegevens. Bijzondere persoonsgegevens zijn vaak 1-op-1 te verbinden aan organisaties. Binnen Europa worden organisaties gecategoriseerd volgens de Europese NACE Rev. 2.'[19] De NACE Rev. 2 bevat een Statistical classification of

[19] Https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF

economic activites in the European Community. Door organisaties te verbinden aan categorieën van bijzondere persoonsgegevens is eenvoudig na te gaan om welke organisaties het gaat. Vervolgens kunnen organisaties binnen deze categorieën het betreffende rekeningnummer op laten nemen in het register. Aanbieders van PSD2 diensten kunnen deze rekeningnummers benutten om bijzondere categorieën van persoonsgegevens uit te zonderen van de verwerking. Wij menen dat het in ieder geval zal gaan om organisaties binnen de volgende categorieën organisaties:

Politieke opvattingen
- **9492** Politieke organisaties

Religieuze of levensbeschouwelijke overtuigingen
- **94911** Religieuze organisaties
- **94919** Beleven, verdiepen en/of verbreiden van een levensbeschouwing niet zijnde een religie

Lidmaatschap van een vakbond
- **9420** Werknemersorganisaties

Gegevens over gezondheid
- **86** Gezondheidszorg. Deze afdeling omvat de groepen:
  - 861 Ziekenhuizen
  - 862 Medische en tandheelkundige praktijken
  - 869 paramedische praktijken en overige ambulante gezondheidszorg
- **87** Verpleging, verzorging en begeleiding met overnachting. Deze afdeling omvat de groepen:
  - 871 Verpleeghuizen
  - 872 Huizen en dagverblijven voor verstandelijk gehandicapten en psychiatrische cliënten
  - 873 Huizen en dagverblijven voor niet-verstandelijk gehandicapten en verzorgingshuizen
  - 879 Jeugdzorg en maatschappelijke opvang met overnachting
- **4773** Apotheken

Ras of etnische afkomst
- Af te leiden uit gedrag zoals zender/ontvanger van bedragen, betalingen aan bepaalde organisaties

Gegevens met betrekking tot iemands seksueel gedrag of seksuele oriëntatie
- Af te leiden uit gedrag zoals zender/ontvanger van bedragen, betalingen aan bepaalde organisaties

De Europese Commissie of het Comité kan het initiatief nemen tot het opzetten van een onafhankelijk register van rekeningnummers, waarbij een transactie van of aan de rekeninghouder, als bijzonder persoonsgegeven gezien kan worden. Binnen ons project PSD2meniet.nl zijn we begonnen met een dergelijk register waarmee we aantonen dat het opzetten en inrichten van een dergelijk register te realiseren is.[20] Daarmee laten we zien dat het mogelijk is een voorziening te treffen zoals u bedoelt in uw punt 57: het verhindert de

[20] https://psd2meniet.nl/gezocht-rekeningnummer-voor-het-register/

opname van bepaalde gegevenspunten en biedt een technische mogelijkheid om bijzondere categorieën van persoonsgegevens uit te sluiten.

Minimaal zou in dit register een voorziening opgenomen moeten zijn voor politieke partijen. Een sluitend overzicht van politieke partijen is af te leiden uit de voor verkiezingen ingeschreven politieke partijen. We wijzen er op dat de huidige bescherming onder artikel 9 AVG waarschijnlijk te weinig bescherming biedt om de doelen van het Internationaal Verdrag inzake burgerrechten en politieke rechten te waarborgen.

XXVII. ***Suggestie***: benoem dat aanbieders van PSD2 een mogelijkheid moeten ontwikkelen om bepaalde categorieën van bijzondere persoonsgegevens uit te kunnen sluiten van een verdere verwerking van persoonsgegevens. Ga er daarbij van uit dat het nu al mogelijk is om de organisaties te duiden waar het om gaat, zoals we hierboven laten zien.

XXVIII. ***Suggestie***: stel minimaal een lijst op van rekeningnummers voor contributies, giften of donaties aan politieke partijen

XXIX. ***Suggestie***: adopteer het PSD2-me-niet register en breidt deze uit.

Ten aanzien van de verwerking van strafrechtelijke gegevens willen we wijzen op een risico dat we zien binnen Nederland, maar mogelijk ook voor andere landen zal gelden. Transacties kunnen herleidbaar zijn tot boetes en daarmee strafrechtelijke informatie onthullen. Op de site van het Nederlandse Openbaar Ministerie staan verschillende overtredingen en bijbehorende boetes. Boetes en andere transacties worden overgemaakt naar één van de 12 openbaar gemaakte rekeningnummers van het administratie kantoor, het CJIB.[21] Een transactie naar één van de nummers onthult een strafrechtelijk gegeven.[22]

Niet alleen kan deze informatie gebruikt worden als onderdeel van een profiel, het kan een bestaande, gereguleerde praktijk omzeilen. De AVG en de 'Uitvoeringswet AVG' bieden ruimte aan private partijen om strafrechtelijke gegevens te gebruiken op grond van artikel 10 AVG. In artikel 33 lid 2 zegt de Uitvoeringswet AVG dat de strafrechtelijke gegevens verwerkt mogen worden door private partijen bij de beoordeling om een beslissing te nemen of een prestatie te leveren, en ter voorkoming van strafbare feiten tegen deze partij. Een duidelijk voorbeeld hoe deze gegevens worden gebruikt zijn de 'Zwarte Lijsten'[23]. Volgens de AP: 'Het doel van een zwarte lijst is om organisaties te waarschuwen voor bepaalde personen. Zo kunnen organisaties beoordelen of zij met die personen zaken willen doen. Bijvoorbeeld of zij die personen in hun winkel willen binnenlaten of in hun hotel willen

[21] https://www.cjib.nl/rekeningnummer

[22] Ook bij zwaardere overtredingen en misdrijven geven boetebedragen veel informatie. Uit de site 'Uittreksel justitiële documentatie' van Justid, de justitiële informatiedienst" (https://www.justid.nl/organisatie/JDS/registratie.aspx) is af te leiden waarvoor boetes uitgedeeld worden. Bij een groot aantal overtredingen krijg je bovendien een strafblad. In het Besluit justitiële en strafvorderlijke gegevens (https://wetten.overheid.nl/BWBR0016544/2018-01-01/#Hoofdstuk2_Afdeling1_Artikel4) is opgesomd welke overtredingen in ieder geval opgenomen worden in de justitiële documentatie (je strafblad).

[23] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten

laten overnachten. Op een zwarte lijst staan vaak strafrechtelijke gegevens of gegevens over ongewenst gedrag.'

Een Zwarte Lijst mag je niet zomaar opzetten. De AP biedt een 'AVG-handleiding protocol zwarte lijst'[24] aan met eisen aan een zwarte lijst. Een zwarte lijst moet voldoen aan formele eisen, algemene informatie over de verwerking zoals de noodzaak voor de verwerking, informatie over de opname van betrokkenen op de zwarte lijst, waarborgen voor de verwerking zoals beveiliging en waarborgen voor de verwerking.

Door PSD2 ontstaat het risico dat aan de hand van bepaalde transacties iemands strafrechtelijke profiel wordt afgelezen. Deze informatie kan een eenvoudig profiel opzetten aan de hand van openbare informatie. Dit kan 'zwarte lijsten' vervangen en daarmee de waarborgen ter bescherming van de fundamentele rechten en vrijheden van de betrokkene omzeilen.

XXX. ***Suggestie***: werk in de richtsnoeren uit hoe strafrechtelijke gegevens uit transactiedata afgelezen kan worden. Benadruk de waarborgen en eisen zoals opgenomen in artikel 10 AVG.

XXXI. ***Suggestie***: Onderzoek of transactiedata, verkregen via een PSD2 dienst, benut mogen worden voor 'zwarte lijsten' op grond van artikel 10 AVG, waarbij belangrijke waarborgen omzeild kunnen worden.

XXXII. ***Suggestie***: benadruk dat strafrechtelijke gegevens uitgezonderd moeten kunnen worden wanneer een betrokkene gebruik maakt van een AISP of gegevens wil benutten voor verdere verwerking, omdat het risico op gebruik voor een strafrechtelijk profiel te groot is.

[24] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg-handleiding_protocol_zwarte_lijst.pdf

8. Gegevensminimalisatie en privacy by design

In uw paragraaf 6.1 legt u op duidelijke wijze uit hoe aanbieders om moeten gaan met dataminimalisatie en privacy by design. Op dit moment is een groot probleem dat consumenten de hoeveelheid bankgegevens niet zelfstandig kunnen beperken of filteren. Zelfs als een financiële dienstverlener bepaalde gegevens niet nodig heeft, wordt na het geven van toestemming toch alle data gedeeld. Vervolgens heeft een consument geen enkele garantie dat een dienstverlener dataminimalisatie doorvoert.

We zien dat aanbieders vaak moeite hebben vast te stellen welke gegevens noodzakelijk zijn voor een verwerking. Vaststellen welke gegevens minimaal benodigd zijn blijkt voor veel aanbieders lastig te zijn of ruimer te worden uitgelegd dan strikt noodzakelijk.

Bij veel diensten is vooraf vast te stellen welke persoonsgegevens verwerkt moeten worden. Een voorbeeld is een risicoanalyse voor het aangaan van een hypotheek, waar bijvoorbeeld een opgave van inkomsten van de afgelopen twee jaar nodig is. Bij veel andere diensten die vaak gemakshalve onder de noemer ‘innovatie’ worden geplaatst, kan de benodigde data niet eens vastgesteld worden of wordt gestreefd naar een zo omvangrijk mogelijke dataset. ‘Eerst de data, dan het denken’ is dan vaak het adagium. Privacy First ziet hier een groot risico omdat het de uitgangspunten van dataminimalisatie op losse schroeven zet. Daarbij kan de verwerking binnen de kaders van de wet geschreven worden terwijl de inrichting van de verwerking toch onnauwkeurig is.

XXXIII. ***Suggestie***: benoem dat aanbieders transparant kunnen zijn (behoren te zijn) over dataminimalisatie en welke ontvangen informatie niet gebruikt wordt, terwijl deze op grond van de wet wel ontvangen kunnen worden.

Op dit moment is de enige partij die bepaalt wanneer sprake is van dataminimalisatie, de aanbieder. Gezien de positie van de betrokkene en het feit dat het zijn of haar gegevens zijn die worden verwerkt kan het Comité aanbieders er op wijzen dat de betrokkene betrokken moet worden bij het vaststellen van welke gegevens deze wil delen. Een goede mogelijkheid bieden verschillende vormen van Persoonlijk Data Management (PDM) waardoor een persoon zeggenschap krijgt over welke gegevens nodig zijn. Zelfs als dat betekent dat bepaalde dienstverlening minder effectief zou zijn.

Ook kunt u in de richtsnoeren wijzen op artikel 35 lid 9 AVG waar expliciet wordt verwezen naar het betrekken van (vertegenwoordigers van) betrokkenen bij het ontwikkelen van verwerkingen en inschatten van risico’s.

XXXIV. ***Suggestie***: bij punt 63 ‘beveelt u aan’ U kunt dit vast duidelijker verwoorden.

XXXV. ***Suggestie***: benoem de mogelijkheid van artikel 35 lid 9 AVG om betrokkenen te betrekken bij DPIA.

Bij punt 62 noemt u een aantal gegevensindicatoren waarvan u vermoedt dat deze snel uitgezonderd kunnen worden. Bijvoorbeeld de identiteit van de stille partij, de transactiekenmerken en het IBAN van de bankrekening van de stille partij. We merken op

dat een AISP ook de mogelijkheid moet bieden om gegevens binnen een categorie uit te sluiten, zoals de categorieën bijzondere persoonsgegevens. Pas dan wordt een zinvolle uitzondering van gegevens mogelijk.

XXXVI. ***Suggestie***: benoem bij uw punt 62 dat dataminimalisatie ook kan inhouden dat categorieën van bijzondere persoonsgegevens worden gefilterd.

9. Profilering

Het hoofdstuk over profilering negeert de grote risico's die samenhangen met profilering. Er is veel onderzoek gedaan naar profilering door creditscorers en databrokers. Nauw verwant aan dit onderwerp zijn de zwarte lijsten. Over deze praktijken schreef *De Groene Amsterdammer* 'U staat op een zwarte lijst'. [25] In 2020 zijn hier weer Kamervragen over zijn gesteld.[26] Andere privacy NGO's zoals Privacy International hebben uitgebreid aandacht besteed aan profiling.[27] Ook in de academische wereld heeft profilering de aandacht, zie bij voorbeeld het artikel 'Profiling and targeting consumers in the Internet of Things provides new challenges for consumers'.[28]

Overweging 28 van de PSD2 geeft voorbeelden van diensten die door AISP's worden aangeboden: "Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment. " De schets geeft een duidelijk beeld van een rekeninginformatiedienst. Een steekproef op de AISP's in het Payment Institutions Register[29] en vervolgonderzoek naar de aanbiedende partijen laat echter zien dat het vaak gaat om business-to-business aanbieders en partijen die een verbinding kunnen maken met kredietbeoordelingen. Deze activiteiten zijn gebaseerd op profilering en zijn anders dan de overwegingen en terminologie van de PSD2 doen vermoeden.

In uw paragraaf 6.5, de punten 79 en verder worden waarborgen rondom profilering genoemd. Deze waarborgen zijn alleen van waarde als een betrokkene zijn of haar gegevens kan terughalen of vernietigen bij verwerkende partijen. Het gaat dan ook om het weghalen van data als onderdeel van profielen én het bijgewerkte profiel. Het profiel of de score kan invloed hebben op een persoon.

XXXVII. ***Suggestie***: wees specifieker over de risico's van profilering

[25] Groene Amsterdammer, editie van 25 oktober 2017, nr. 43 over De schuldenindustrie 'U staat op een zwarte lijst'. https://www.groene.nl/artikel/u-staat-op-een-zwarte-lijst (2017).
[26] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?did=2020D34917&id=2020Z16169
[27] www.privacyinternational.org
[28] https://www.ivir.nl/publicaties/download/1747.pdf
[29] https://euclid.eba.europa.eu/register/pir/search

XXXVIII. ***Suggestie***: benadruk dat betrokkenen van wie een profiel wordt gemaakt, langdurig impact kunnen merken van de profilering. Benadruk dat partijen aan hun informatieplichten moeten voldoen.

XXXIX. ***Suggestie***: benoem dat als een betrokkene bij een verzoek tot verwijdering, of bij het actief intrekken van toestemming, dat brondata waarmee profielen worden opgesteld ook verwijderd moeten worden en dat de profielcodering moet worden aangepast op basis van de gewijzigde data.

XL. ***Suggestie:*** benoem voorbeelden die meer recht doen aan de praktijk van AISP, die meer verwerken dan is beschreven in overweging 28 PSD2.

10. Tot slot

We wensen u veel succes met de volgende versie van de Richtsnoeren. We zijn altijd bereid om onze opmerkingen en aanbevelingen nader toe te lichten. Tenslotte verwijzen we u nogmaals naar onze website PSD2meniet.nl voor aanvullende informatie over ons project en activiteiten.

Met vriendelijke groeten,

Martijn van der Veen
Stichting Privacy First
Woordvoerder PSD2

Vincent Böhre
Stichting Privacy First
Directeur